Grant Thornton

2023-2024

Cybersecurity in Canada

Contents

The story so far

When discussing cybersecurity, the only constant is the ongoing escalation of threat and response that sees both attackers and defenders evolve their tactics. As attackers exploited new vulnerabilities driven by the continued growth of remote work and the expansion of the internet of things (IoT), defenders responded with artificial intelligence (AI) security solutions and zero-trust architectures. However, as we'll see, just because new threats emerge doesn't mean the old threats fade away. Long-term challenges such as social engineering continue to threaten both businesses and individuals.

Smaller businesses under attack

With larger organizations typically having strong controls around cybersecurity, whether in terms of training, processes or technology, small- and medium-sized businesses (SMBs) are increasingly feeling the brunt of cyber-attacks in Canada. As these businesses increasingly relied on digital infrastructure for day-to-day operations, they became enticing targets for cybercriminals seeking to exploit vulnerabilities. Phishing attacks, ransomware incidents, and data breaches were among the most prevalent threats faced by SMBs. Many of these smaller Canadian businesses lacked the resources and expertise to implement robust cybersecurity measures, making them more susceptible to exploitation.

The financial repercussions of cyber-attacks were often devastating for small businesses, with the cost of recovery and reputational damage putting their very survival at risk. The average cost of a data breach in Canada is $5.64 million—$1 million more than the global average and a Mastercard study showed that 99% of victims said the cyber-breach impacted their business operations. Furthermore, the study noted that the most common effect of these cyber-breaches was the loss of customer data, and more than a third said the hack strained their relationships with vendors or customers.

Moreover, the interconnected nature of supply chains meant that small businesses often became entry points for larger-scale attacks on their partners and customers. In response to this escalating threat, industry experts and governments stressed the importance of raising cyber awareness and providing support to small businesses in enhancing their cybersecurity posture. Collaborative efforts between cybersecurity firms, governments, and trade associations aimed to equip small enterprises with the necessary tools and knowledge to defend against cyber threats, empowering them to navigate the digital landscape with greater resilience and confidence.

The average cost of a data breach in Canada is

$5.64 million

The weakest link in the (supply) chain

Supply chain attacks provide an indirect method for attackers to breach a target organization. By first compromising a supplier and subsequently exploiting their trusted relationships with downstream organizations, threat actors can entirely circumvent those organizations' secure network perimeter, thus avoiding the need for direct action against a target network's defenses. Many of the attacks we've seen in recent years have come via weak third and fourth parties with the methods used to provide remote access to these organizations found to be insecure. A Gartner risk report indicated that,

"There were 100 times more supply chain attacks in 2022 than in 2020. This trend will only get worse—by 2025,

45% of global organizations will be impacted."

This vulnerability has led to an increased emphasis on third-party risk management. Security audits of potential external vendors and partners are becoming standard fare in the vetting process. Companies that are unable to demonstrate a solid security approach are losing business. As a result, many companies are prioritizing employee awareness and training programs. As the threat landscape continues to evolve, collaboration and information sharing within industries and regulatory bodies have become essential to stay ahead of cyber adversaries. The future of supply chain cyber security lies in adaptability, resilience, and a proactive approach, ensuring that businesses can thrive in the face of the ever-changing cyber threat landscape.

Battling burnout—overcoming cyber fatigue

Cybercriminals continued to look for the easiest ways to access an organization's network or systems—the quickest and cheapest path that allows them to stay hidden under the disguise of an authorized employee. We saw continued growth in attacks perpetrated by social engineering, which contributed to fraud hitting all-time-high in Canada. In 2022, fraud cost Canadians at least $530 million, a 40% jump over the previous according to the Canadian Anti-Fraud Centre.

As the scope and number of attacks increased, cyber-fatigue emerged as a pressing concern within the technology and security communities. An unprecedented surge in cyber-attacks, data breaches, and privacy violations, led to a constant barrage of security alerts, updates, and notifications for individuals and organizations alike. Additionally, the spike in attacks has seen security teams impose an overwhelming number of precautions on workers: use extremely long and complex passwords, change them every six weeks, multi-factor everything, keep your systems updated, and never, ever use insecure Wi-Fi. As a result, there was a noticeable sense of exhaustion among users (and security professionals). The continuous stream of cybersecurity news and incidents also contributed to a desensitization to the severity of the threats, making it challenging to distinguish genuine risks from noise.

Cyber-fatigue manifests as decreased vigilance, complacency towards security measures, and a higher likelihood of falling victim to social engineering tactics.

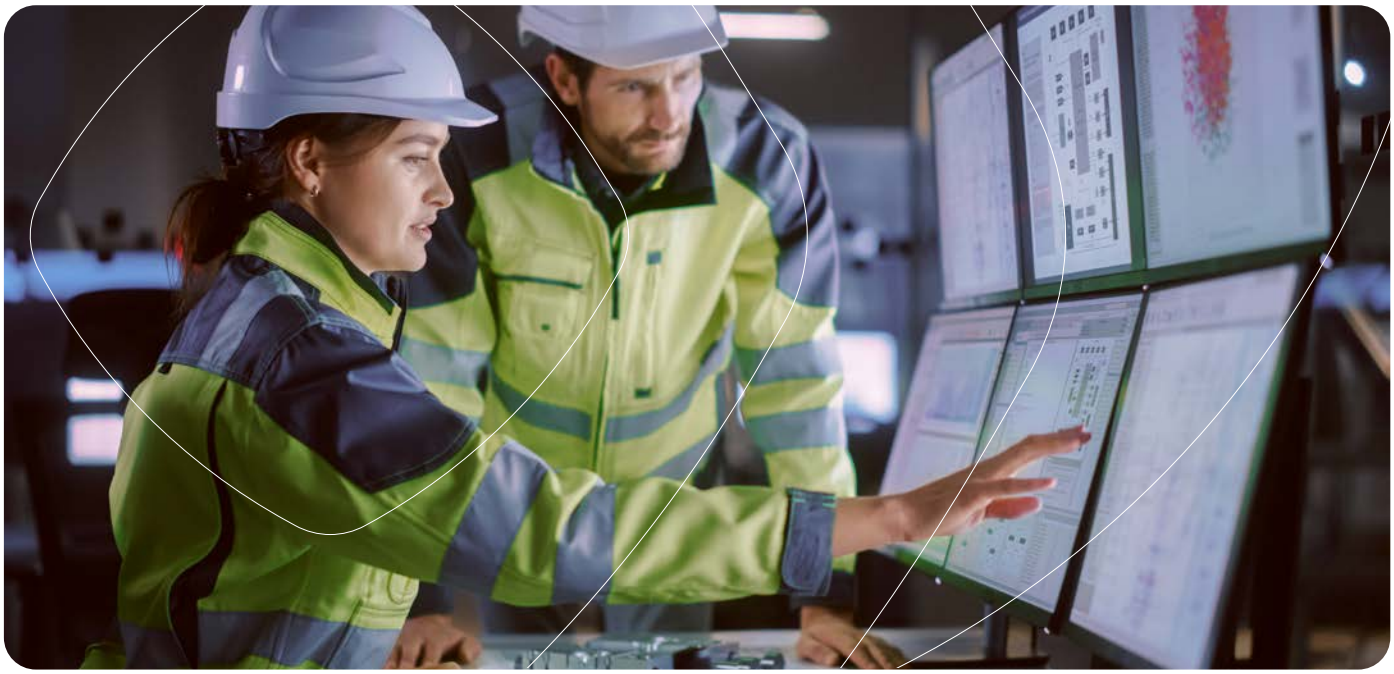
Addressing cyber fatigue became a critical aspect of cybersecurity strategies, necessitating user-friendly security interfaces, clear communication of risks, and efforts to strike a balance between security measures and usability. In 2022, the industry recognized the importance of not only fortifying technological defenses but also fostering a cybersecurity culture that acknowledges the impact of fatigue and empowers individuals and organizations to remain vigilant and resilient in the face of evolving cyber threats.

Overall, the past year has proved pivotal year for cybersecurity, emphasizing the necessity for constant innovation and adaptability to protect against emerging threats in an increasingly interconnected digital landscape.

In 2022, fraud cost Canadians at least

$530 million

Trends on the rise



Attacks on critical infrastructure

Cyber-attacks on critical infrastructure and Operational Technology (OT) systems are a growing concern due to their potential to cause severe disruptions and catastrophic consequences. As nations continue to digitalize and interconnect their essential services, attackers increasingly view critical infrastructure as attractive targets.

This trend has been consistently growing for years, but took on new urgency with the ongoing war in Ukraine. Cyber warfare has emerged as a powerful tool used by state and non-state actors to achieve their strategic objectives. The conflict has witnessed an increase in sophisticated cyber-attacks targeting critical infrastructure, government institutions, and private organizations, both within Ukraine and beyond its borders. Canada is not immune to this. As a NATO member providing ongoing support for the Ukrainian government we have been a target for attacks on critical infrastructure such as our energy system. A recently published Communications Security Establishment (CSE) threat assessment noted that "*…this activity is very likely to disrupt critical services for psychological impact, ultimately to weaken Canadian support for Ukraine. We assess that this activity will almost certainly continue for the duration of the war, and will likely increase as Russia's invasion efforts falter, or new support for Ukraine is announced.*"

The situation in Ukraine serves as a important reminder of the potential effects of cyber warfare on a global scale. It highlights the importance of enhancing cyber security measures not only for nations involved in armed conflicts but for the international community as a whole.

Some key trends in cyber-attacks on critical infrastructure and OT in 2023 include:

- **Advanced threats:** Cyber attackers are using more sophisticated tactics, techniques, and procedures to target critical infrastructure. These attacks involve advanced malware, zero-day exploits, and multi-stage campaigns that aim to evade detection and cause maximum damage.
- **Ransomware targeting infrastructure:** Ransomware attacks have evolved to specifically target critical infrastructure, such as power grids, water facilities, and transportation systems. The attackers' goal is not only to encrypt data but also to disrupt operations and extort large ransom payments.
- **Supply chain attacks:** Attackers may exploit vulnerabilities in the supply chain of critical infrastructure, compromising trusted vendors and suppliers to gain unauthorized access to critical systems and data.
- **Convergence of IT and OT:** As IT and OT systems converge to increase efficiency and connectivity, the attack surface for critical infrastructure expands, offering attackers more entry points into the industrial control systems.

To counter these threats, critical infrastructure operators are investing in state-of-the-art cybersecurity technologies, conducting regular risk assessments, and prioritizing employee training to improve cyber awareness. Furthermore, comprehensive incident response plans and continuity strategies are being implemented to reduce downtime and mitigate the potential impact of successful cyber-attacks.

As the world becomes increasingly reliant on interconnected systems, the focus on protecting critical infrastructure and OT from cyber threats will remain a top priority for both public and private sectors.

AI: the double edged sword

The continued adoption of AI holds immense promise for various industries, but it also comes with significant cybersecurity implications. AI's widespread integration in diverse applications, from autonomous vehicles and smart cities to healthcare and finance, enhances efficiency, decision-making, and user experience. However, this increased reliance on AI-driven systems opens up new attack vectors and potential risks that need to be addressed to ensure a secure digital landscape.

One major cybersecurity implication is the potential for AI-generated cyber-attacks. As AI technologies advance, cybercriminals can leverage them to create more sophisticated and targeted attacks, such as AI-powered phishing campaigns, deepfake attacks, and automated malware generation. These attacks can be difficult to detect and respond to, as they may mimic legitimate user behavior and exploit AI-based vulnerabilities in systems. Moreover, AI-driven cyber-attacks can lead to more significant and widespread impacts. Automated and highly scalable attacks could potentially disrupt critical infrastructure, financial markets, or even influence political processes. The use of AI by malicious actors may also blur the lines between cyber warfare and cybercrime, creating complex challenges for attribution and response.

Another cybersecurity challenge is related to the security of AI systems themselves. As AI algorithms become increasingly complex and interdependent, they become vulnerable to adversarial attacks and data poisoning. If attackers can manipulate the training data or input to AI systems, they can lead to biased decisions, misclassification, or unauthorized access to sensitive information.

Additionally, the shortage of skilled cybersecurity professionals capable of effectively defending against AI-driven threats is a growing concern. The demand for AI expertise in both offensive and defensive capabilities may outpace the availability of skilled personnel, leaving organizations vulnerable to emerging cyber threats.

Collaboration between the cybersecurity community, policymakers, and AI developers will be essential in order to establish ethical guidelines, standards, and regulations to ensure the responsible and secure deployment of AI technologies in the years to come.

Insurance providers react to growing risks

A surge in online attacks has had a profound impact on the insurance landscape, sparking a reevaluation of business' risk management strategies and prioritization of cyber insurance as a crucial component of their overall security posture.

As cyber threats continue to diversify and become more sophisticated, cyber insurance policies will likely expand to cover a broader range of risks. This may include coverage for emerging threats like AI-driven attacks, supply chain vulnerabilities, and cyber-physical risks (e.g., attacks on IoT devices impacting physical infrastructure). It may also mean offering tailored and dynamic policies where insurers may offer more customized and dynamic cyber insurance policies tailored to specific industries, business sizes, and risk profiles. These policies may be designed to adjust their coverage and premiums based on real-time risk assessments and the insured entity's cybersecurity posture.

However, rates have skyrocketed as insurance providers cope with high payouts. The Insurance Bureau of Canada (IBC) noted that over the past three years, insurers paid out $2.30 in cybersecurity claims and operating expenses for every dollar earned in premiums, an unsustainable situation for insurance providers. Business leaders are looking to mitigate the risks from cyberattacks and ransomware, which for many has been devastating both in terms of business availability and financial stability. The need to reduce the financial burden of cyberattacks has seen many business leaders look to the cyber insurance industry as a safety net. In many cases, Canadian organizations have found that the cost of premiums and/or the implementation of the requirements specified by insurance companies was either out of reach from a budget perspective or it made more sense to focus those funds directly on securing their infrastructure.

As cyber-attacks became more disruptive and costly, insurance providers adapted their offerings to address the evolving threat landscape. However, the increased risk also led to a reevaluation of policy terms and premiums, with some insurers tightening their underwriting criteria to mitigate potential losses. The growing demand for cyber insurance led to an expansion of the market, with new insurers entering the arena and existing ones refining their coverage options. The year saw a greater emphasis on tailored policies, where businesses could customize coverage based on their specific needs and risk exposure. Additionally, the cyber insurance industry focused on providing proactive risk assessment and incident response services to help organizations bolster their cyber resilience.

Insurance providers payout

$2.30 for every $1.00 in premiums

Incentivizing cybersecurity—the future of insurance terms

As cyber threats evolve, insurance will play a crucial role in helping individuals and organizations navigate the complexities of the digital age and manage the financial repercussions of cybersecurity incidents.

Even as insurance providers innovate to develop new risk mitigation products, organizations should also expect higher scrutiny over the maturity of their cybersecurity controls and requirements for more detailed cybersecurity risk assessments from policyholders to determine the level of coverage and premiums. Entities with stronger cybersecurity measures may receive more favorable premiums, while those with higher risk profiles may face increased costs. This could encourage businesses to improve their cybersecurity practices to qualify for better coverage terms.

To mitigate both cybersecurity risk and the financial risk of high insurance premiums, businesses must prioritize cybersecurity measures such as implementing robust security protocols, conducting regular security assessments, investing in employee training, and staying informed about the latest threats and best practices in the industry. Collaboration with cybersecurity experts and leveraging advanced threat detection technologies can also help organizations fortify their defenses against the evolving cyber threat landscape.

Zero trust: Never trust, always verify

The concept of zero trust is becoming increasingly vital in the field of cybersecurity. Traditional security approaches that relied on perimeter-based defenses are no longer sufficient to protect modern, dynamic digital environments. Zero trust architecture offers a paradigm shift by assuming that no entity, whether internal or external, should be trusted by default. Instead, it advocates verifying and validating every access request and transaction, regardless of the user's location or device.

The importance of zero trust lies in its ability to address the evolving threat landscape. With the rise of remote work, cloud computing, the attack surface has expanded, making it more challenging to establish a secure perimeter. Zero trust embraces the "never trust, always verify" principle, reducing the risk of lateral movement for cyber attackers within a network. This model helps prevent data breaches and unauthorized access even if the attacker has already compromised one part of the system.

Additionally, zero trust fosters a more granular and context-aware approach to access controls. Identity and access management (IAM) solutions become more sophisticated, utilizing continuous authentication, multi-factor authentication (MFA), and adaptive access policies based on user behavior and device health. This enhanced visibility and control make it easier to identify suspicious activities and respond promptly to potential security incidents.

Moreover, the zero-trust philosophy emphasizes data protection. By adopting encryption and tokenization, data remains secure even if it falls into the wrong hands. This approach helps businesses comply with regulatory requirements and maintain customer trust.

As cyber threats continue to evolve, the concept of zero trust is poised to become a foundational pillar of cybersecurity strategies. Its adaptive, proactive, and context-aware nature makes it an essential approach to safeguard digital assets, privacy, and sensitive information.

Embracing future challenges and opportunities

As the cyber threat landscape continues to evolve with increasingly sophisticated attacks and emerging technologies, the need for robust cyber defenses has never been greater. Organizations and individuals alike must remain vigilant, proactive, and adaptable to the dynamic nature of cyber threats. Embracing advanced technologies such as AI-driven security solutions and zero-trust architectures will become crucial in safeguarding digital assets and personal information. Collaboration between industry stakeholders, governments, and cybersecurity experts will pave the way for more effective threat intelligence sharing and coordinated response efforts. Furthermore, a strong focus on cybersecurity awareness and education will empower individuals to protect themselves against cyber risks. Despite the complexity of the challenges ahead, the collective commitment to cybersecurity will lead to a safer digital landscape, where innovation and technology can thrive securely.

Organizations must continue to shift their focus on creating a culture of cybersecurity—following breaches such as Sobeys, we will hopefully see that good security culture will continue to become the norm for organizations that have received ongoing security awareness training. With risk exposure (company reputation, revenue, and growth) being a top issue for cybersecurity, expect boardrooms to make cybersecurity a top priority.

Peter Morin

Principal
National Cybersecurity Leader

About the author

With over 25 years of experience, Peter's unique expertise ranges from industrial and control system (ICS) security, network security architecture, threat hunting and red-teaming to cloud security, incident response and computer forensics.

Peter has held senior positions with numerous organizations, including a global cybersecurity consulting firm, a national telecommunications and media company, a Fortune 500 cloud-computing company, a recognized cybersecurity software company and a major US defense contractor.

Peter is originally from Montreal, and now lives with his family in Halifax, Nova Scotia.

Peter Morin
Peter.Morin@ca.gt.com
+1 902 421 1734

Grant Thornton

grantthornton.ca

Audit | Tax | Advisory

About Grant Thornton LLP in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide.